Exhibit 4

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND/ODESSA DIVISION

MALIKIE INNOVATIONS LTD.,
KEY PATENT INNOVATIONS LTD.
Plaintiff,
v.
MARA HOLDINGS, INC.
(F/K/A) MARATHON DIGITAL HOLDINGS, IN
Defendant. CIVIL ACTION NO.
7:25-cv-0022-DC-DTG

VIDEOTAPED DEPOSITION OF DR. ÇETIN KAYA KOC

DATE: Friday, January 9, 2026

LOCATION: Via Zoom

REPORTED STENOGRAPHICALLY BY:
Jennifer Miller, RMR, CRR, CCR-NJ,
CCR-WA, CCR-NM, CALIFORNIA CSR#14652
Notary Public: NJ, NY, PA, DE

2

APPEARANCES

REICHMAN JORGENSEN LEHMAN & FELDBERG
BY: PHILIP EKLEM, ESQ.
1909 K Street, NW, Suite 800
Washington, D.C. 20006
202.894.7451
peklem@reichmanjorgensen.com
Counsel on behalf of Plaintiffs, Malikie Innovations and Key Patent Innovations

PAUL WEISS
BY: ANISH DESAI, ESQ.
PRIYATA PATEL, ESQ.
1285 Avenue of the Americas
New York, NY 10019-6064
212.373.3394
adesai@paulweiss.com
Counsel on behalf of the Defendant, MARA Holdings, Inc. and the witness

Also present: Joe Cerda, Videographer

3

INDEX

4

PROCEEDINGS

THE VIDEOGRAPHER: We are on the record. This is a remote video deposition of Dr. Çetin Koc in the matter of Malikie Innovations Limited, et al., versus Mara Holdings.

My name is Joe Cerda. I am the video technician today. The Court Reporter is Jennifer Billstein. We both represent Digital Evidence Group.

Today's date is January 9, 2026. The time on the record is 8:07 a.m.

Will all parties please identify themselves for the record and who they represent.

ATTORNEY EKLEM: This is Philip Eklem with Reichman Jorgensen Lehman & Feldberg on behalf of plaintiffs Malikie Innovations and Key Patent Innovations.

ATTORNEY DESAI: Anish Desai and Priyata Patel from Paul Weiss on behalf of the defendant, MARA, and the witness, Dr. Koc.

THE WITNESS: Çetin Kaya Koc, expert witness, on this current matter mentioned.

5

ÇETIN KAYA KOC, after having been first duly sworn, was examined and testified as follows:

- - -

EXAMINATION

- - -

BY ATTORNEY EKLEM:

Q. Thank you. Good afternoon to you, Dr. Koc. Good morning to everyone else.

Would you mind, just go ahead and just please state your record -- state your name for the record now that we're on.

A. Çetin Kaya Koc. Koc is my last name.

Q. Yes. Thank you, Doctor.

Have you ever been deposed before, Dr. Koc?

A. Yes.

Q. How many times?

A. I believe three times.

Q. Were any of those times related to patent litigation or patent matters?

A. Patent matters, all of them.

Q. Okay. Do you recall the technology at issue in those three cases?

6

A. They were related to cryptographic products, engineering, hardware, software.

Q. For those three cases, if you can remember, do you know if you represented the patent owner or the patent challenger? Do you recall?

A. In one case, it was the patent owner. In another case, it was a challenger. Finally, in another case, it was a challenger.

Q. Thank you.

Have you ever testified in -- at a trial before?

A. I have been invited to PTAB for testifying but never asked. And, no, I have not in person.

Q. And you understand that you're under oath today, which means that you must provide truthful and accurate testimony as if you were testifying in a courtroom?

A. Of course I do.

Q. Okay. So this deposition will be basically a question-and-answer session between you and me where I'll ask the questions and you'll give the answers. So unless your attorney instructs you not to answer, you are

7

to answer my questions.

Do you understand?

A. I do.

Q. Okay. And if any of my questions are not clear, if you don't understand, just ask me to clarify. And I'll do my best if I can.

Is that all right?

A. That's right.

Q. Okay. Now, during the course of the deposition, your attorneys may object to my questions; but unless they instruct you not to answer after their objection, you can go ahead and answer my questions.

Do you understand?

A. Yes.

Q. Okay. So I think we'll, you know, probably take a break about every hour. But, of course, if at any time during the deposition you need to take a break, let me know. And I'll try to quickly get us to a place where we can do that. Okay?

A. All right.

Q. So I'm going to ask you to please refrain from engaging in any forms of electronic communication during the deposition,

8

so emails, texting, you know, Teams and all that stuff, while we're on the record, if you don't mind just leaving those things aside. Okay?

A. Of course.

Q. Great.

Other than the Zoom program and the Box program for the exhibits, do you have any other programs open on your computer in front of you?

A. None.

Q. Okay. And where are you located today, Dr. Koc?

A. I am located near Barcelona, Spain.

Q. Okay. Is anybody else in the room with you today?

A. No.

Q. Is there any reason why you would not be able to answer my questions truthfully and accurately today?

A. I don't see any reasons.

Q. Okay. Are you taking any medications that might affect your ability to testify truthfully?

A. No.

9

Q. Great.

ATTORNEY EKLEM: So let's go ahead and put in Exhibits 1 and 2.

Joe, if you want to put in documents 1 and 2, please.

- - -

(Whereupon, Exhibit 1 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. This will be your declaration and errata.

- - -

(Whereupon, Exhibit 2 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. When that's available to you, Dr. Koc, please let me know.

THE VIDEOGRAPHER: Philip, you want to mark those as Exhibits 1 and 2 as well?

ATTORNEY EKLEM: Yes, please.

THE VIDEOGRAPHER: Stand by.

ATTORNEY DESAI: Philip, just so

10

you know, Dr. Koc has a paper copy of his declaration. And he also has a binder with a paper copy of all of the exhibits that are referenced.

ATTORNEY EKLEM: Okay.

BY ATTORNEY EKLEM:

Q. Dr. Koc, other than your binder that contains your declaration and exhibits, do you have any other papers or notes with you today?

A. No, I don't.

Will you be sharing the documents over the Zoom as document sharing, or do I need to go to the Box and get it?

Q. We will do both. So Joe is going to put them up, and he'll follow along with what I'm saying. But you can also access them directly, and sometimes it is easier, I think. It may be easier at times for you to download whatever document it is so you can, you know, have control of the navigation. But we will -- we can do both.

A. Okay.

Q. All right. So what we have here is Exhibit -- I'm sorry?

ATTORNEY DESAI: Dr. Koc, you

11

can also feel free to use the paper copies you have as well.

THE WITNESS: Yeah. I do have a paper copy of everything.

BY ATTORNEY EKLEM:

Q. Yes. Right. So then that's totally fine, too.

So let's -- so what we've entered as Exhibits 1 and 2 is your declaration and your errata.

Let's start with Exhibit 1. So if you want to pick up your declaration, please, Dr. Koc.

And the first page is Exhibit A, but if you want to go the page -- the next page with the case caption.

A. Okay.

Q. I just want to confirm a few things here. So the title is [as read]:

"Expert Declaration of
Dr. Çetin Kaya Koc in Support
of MARA's Opening Claim
Construction Brief."

Do you see that?

A. Yes.

12

Q. If you go to the very end of the document, the very last page, you should see a signature and a date, January 7, 2026.

Do you see that?

A. Yeah.

Q. I just want to confirm. That's your signature?

A. Yes, it is.

Q. Great.

A. It's not January. It's December 17th.

Q. I'm sorry. Yeah. I don't know what I said. The date is December 17, 2025.

So -- so you can confirm this is -- this is the declaration that you submitted -- Exhibit 1 is the declaration that you submitted in this case in connection with the -- MARA's claim construction brief, right?

A. Right.

Q. Okay. And this declaration, does it contain your opinions?

A. Yes.

Q. And you stand by all the opinions in your declaration?

A. I do.

13

Q. Other than the errata, which is in Exhibit 2 -- and feel free to take a look at that if you'd like.

Other than that errata, is there anything about your declaration that you want to change or correct today before we get started?

A. No.

Q. Okay. So let's go to paragraph 15 of your declaration, please. That is on -- that's on page 5.

A. Yeah.

Q. It says that a copy of your CV is attached as Appendix A.

Now, I don't -- I don't think there was an Appendix A attached, but I do have a copy of your CV that we received from counsel.

ATTORNEY EKLEM: Joe, could you enter Document 3, please, and mark it as an exhibit, which will be Exhibit 3.

- - -

(Whereupon, Exhibit 3 was marked for identification.)

- - -

14

BY ATTORNEY EKLEM:

Q. So, Dr. Koc, what we put up here on the screen and what should also be available in the Box to you is a copy of the CV that we received.

Can you confirm that this is a copy of your CV?

A. It is, starting from first page. I'm assuming the rest of it would be correct too.

Q. Okay. If you want to take a minute to look through, we can -- you can download it. But I'll represent that this is the copy that we received from your counsel.

A. Yes. 26 pages, all correct.

Q. Okay. So then let's go back to your declaration now and go to paragraph 6, please.

A. Yeah.

Q. In paragraph 6, it says that you're a retired research professor in the department of computer science at UCSB, right?

A. True.

Q. When did you retire from UCSB?

A. 2024, June.

Q. And before UCSB, you were previously a professor at Oregon State University,

15

correct?

A. Correct.

Q. Taking a look down at paragraphs 7 and 8, both of those paragraphs refer to cryptographic engineering.

Do you see that?

A. Yes.

Q. What is cryptographic engineering?

A. The development of cryptographic products in hardware and software form and all of the technologies, algorithms, methods related to it.

Q. Okay. Would you say that cryptographic engineering is a multidisciplinary field?

A. Indeed. In my talk, I always say it encompasses electrical engineering, computer science, and mathematics.

Q. Okay. You said electrical engineering, computer science, and mathematics, correct?

A. Correct.

Q. Great.

So let's go on down to paragraph 14 on page 4.

16

A. Yes.

Q. Paragraph 14 indicates that you coauthored five books, correct?

A. True.

Q. Would those books provide a reliable source of information for understanding the concepts addressed in your declaration?

A. Yes, they do.

Q. Okay. So let's go on down to paragraph 22 on page 7.

A. Yeah.

Q. Paragraph 22 includes your definition of the person of ordinary skill in the art, which is the acronym POSITA, P-O-S-I-T-A.

Do you see that?

A. Yes.

Q. Would the person of ordinary skill in the art need to be a cryptographic engineer, in your opinion?

A. Not necessarily, but study cryptography, among other subjects like hardware and software.

Q. Would they need to be able to design, implement, test, and validate cryptographic systems to be a person of ordinary skill?

17

A. They would have to be involved but not necessarily alone doing that.

Q. When you say "not necessarily alone," do you mean that they might be working with or collaborating with others that have helpful knowledge?

A. True, yeah. Collaborating with others who have overlapping knowledge of those fields, so, therefore, designing a system together.

Q. So the person of ordinary skill would have some knowledge in mathematics, computer science, and electrical engineering?

A. Not all three, but at least in one of them.

Q. Okay. All right. Let's go to paragraph 25 on the next page, page 8.

A. Yeah.

Q. In paragraph 25, about in the middle-ish -- yeah, about in the middle of the paragraph, there's a sentence that begins with [as read]:

"The mod operation is often referred to."

Do you see that?

Page 18

A. Yes.

Q. It says [as read]:

"The mod operation is often referred to as 'modular reduction' or 'reduction,' because it 'reduces' the value of a number larger than the modulus to below the modulus."

Do you see that?

A. Yes.

Q. Is reducing the value of a number larger than the modulus to below the modulus the same thing as reducing to a specific finite field?

A. I may ask a clarification about which finite field it is, yes.

Q. Okay. It would be -- well, let's take one scenario where the modulus is -- well, let me ask you a question about your question.

When you say "which finite field it is," what kind of information are you looking for? I mean, are you asking what the specific modulus is? Are you asking for a definition of -- a definition of the finite field? What would be helpful?

Page 19

ATTORNEY DESAI: Objection to form.

THE WITNESS: The previous two sentences and today one that you highlighted, the yellow, defines a very particular finite field involving numbers from zero to n minus one. So the context here of the modular reduction context is for that kind of finite fields, which is a finite field consisting of numbers between 0 and n minus 1. Those are integers. And so, therefore, the module operation here would be limited or would be referring to in that kind of field.

BY ATTORNEY EKLEM:

Q. Okay. Whenever you're doing a mod operation of this type, though, aren't you always using a defined finite field? Maybe not the same finite field as in your example, but wouldn't the finite field always be defined?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Well, you're always working in a very particular finite field whose definition is given by the

Page 20

parameters of that finite field.

BY ATTORNEY EKLEM:

Q. Okay. So then in your -- in your paragraph 25 -- so in your paragraph 25, performing a mod n is reducing to a specific finite field, right?

A. In paragraph 25, a mod n and all those four sentences in this paragraph refers to that particular finite field. Then it is to that finite field, meaning if it is to get modular n.

Q. Okay. Let's go to paragraph 31, please, on page 10.

A. Yes.

Q. So paragraph 31 begins with [as read]:

"One fundamental theorem of modular arithmetic is that, for addition, subtraction, and multiplication, 'reducing each intermediate result' with field modulus n 'gives the same answer as computing in ordinary integer arithmetic and reducing the result

Page 21

mod n.'"

Do you see that?

A. Yes.

Q. So here you're identifying two techniques where one technique is reducing each intermediate result and the other technique is not reducing each intermediate result but doing one result -- one reduction at the end, correct?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Exactly what you're asking here?

BY ATTORNEY EKLEM:

Q. What I'm asking is the description that you provide at the beginning of paragraph 31 identifies two ways to do reduction, correct?

ATTORNEY DESAI: Objection to form.

THE WITNESS: This particular paragraph is from a prior art of well-known book. And, essentially, it says you can reduce the temporary results and then compute the final results, or you

22

can continue -- compute the final results without reduction. You would obtain the same value.

BY ATTORNEY EKLEM:

Q. Okay. So in other words, if you do it one way, you get a result; and if you do it the other way, you get the same result, correct?

ATTORNEY DESAI: Objection to form.

THE WITNESS: If you do it one way, you get that result. If you do it the other way, you get another result, which are modularly equivalent. That's what it's saying.

BY ATTORNEY EKLEM:

Q. Okay. Is there -- is it possible to reduce only some of the intermediate results and also do a final reduction at the end as a third option?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Any scenario is possible. Some of it, all of it, a quarter of it could be reduced during the

23

operation.

Each time you would get a different number. Still, they would all be equal to one another, modular n.

BY ATTORNEY EKLEM:

Q. Okay. So let's take a look at paragraph 32. You provide a couple of examples here.

A. Yeah.

Q. In the -- in the example that you describe that reduces the intermediate results, the modulus here is 97, correct?

A. Correct.

Q. And it's true that 50 mod 97 is 50 and 25 mod 97 is 25, correct?

A. Correct.

Q. So in the fourth line of your example, where it shows the four mod operations inside the brackets, technically you would not need to do the last two on 50 and 25, correct?

A. If you do it by hand, you can skip it as a human, but the computer would still have to go through the process of reduction.

Q. Okay. So if you're doing it on a computer -- I see.

24

So you're saying that if you did it on a computer, you could not skip it. You would necessarily have to do all of the intermediate reductions?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Depending on the code that performs the -- program that performs the reduction, it would receive the input and would go through -- the steps of the code would produce the output. In this particular case, it would receive 50 and it would give out 50.

BY ATTORNEY EKLEM:

Q. Okay. So can you -- can you think of a scenario where -- using a computer to do the computations, can you think of a scenario where only some of the intermediate results need to be reduced, but not all of them?

ATTORNEY DESAI: Objection to form.

THE WITNESS: I can think of a program that would check the input. If it's already less than n, it would just simply output it. And I could think of a

25

program like this, and that's sensible.

BY ATTORNEY EKLEM:

Q. Okay.

Okay. So let's go to paragraph 34 on page 11, please.

A. Yes.

Q. In the second sentence, it says [as read]:

> **"A finite field is a field having a finite number of elements."**

Do you see that?

A. Yes.

Q. Now, you have Footnote 1 at the bottom of the page that then says [as read]:

> **"A field is a set of numbers with the usual operations of addition, multiplication, and division and all the usual algebra rules hold."**

Do you see that?

A. Yes.

Q. So does that mean finite field elements are always numbers?

Page 26

A. The finite field elements could be numbers. The finite field -- there are finite fields with elements that are polynomials. There are finite fields whose elements are more complex than polynomials. But, yes, in this particular case, Fp prime field would be numbers.

Q. Okay. Let's go to paragraph 44, please, on page 14.

A. Yes.

Q. Okay. The first sentence in paragraph 44 says [as read]:

> **"Performing Montgomery reduction involves first adding to the reductant a carefully chosen integer multiple of the modulus (i.e. T plus m times n) such that the sum becomes divisible by the radix R equals 2 to the power of k."**

Do you see that?

A. Yes.

Q. Okay. So why do you want the sum to be divisible by R?

Page 27

A. The Montgomery algorithm -- the Montgomery reduction algorithm was invented in 1985. It was not known before. But since then, we've learned there's a very fast way to do reduction using Montgomery's algorithm.

Specifics of that algorithm, algorithmic details, mathematics is part of that sentence that tells you how it needs to function.

Q. So in Montgomery's algorithm, the -- you add -- you add a multiple of the modulus to the reductant, and the goal of doing that is to cause the modified reductant to become divisible by R; is that right?

A. In one of the steps, yes, but allowing division by R allows you to make the number smaller, smaller and, therefore, you reduce the number from below to a number less than n. And that's your goal in Montgomery reduction.

Q. So how does dividing by R cause the number to become smaller or lower, as you said?

A. In a computer, R is the power of 2. Dividing by R implies shifting the number to right. R is 2 to 3k means k bits, the number

Page 28

shifted to right. If the number was 10 bits, it would shift it to right. If 4 bits, the number becomes 6 bits, which is now a smaller number.

Q. Is there a way to perform the computation in the computer of dividing by R without -- without simply shifting?

A. No, no reason to do the other way because the simpler way is already available to you.

Q. But is there another way, I guess, is my question.

A. If you try to divide by R, you end up shifting -- shifting it to right, period.

Q. Meaning the same thing happens? Is that what you mean?

A. Yeah. And you end up with the same result in fact going through the same steps.

Q. This paragraph continues onto the next page.

A. Yeah.

Q. In the last sentence of the paragraph at the -- yeah. At the very end of the paragraph, it says [as read]:

> **"This ensures that the**

Page 29

> **result is in fact T times R to the minus 1 mod n."**

Do you see that?

A. Yes.

Q. The T in that expression, that is the modified reductant, right, not the original?

A. The T is the original T.

Q. T is the original --

A. Original T and R inverse is stuck to it, is multiplied with it; you get that result. And that result would be less than that.

Q. Okay. So must the radix, the R value in Montgomery reduction, necessarily be the power of 2?

A. In the computer implementation where every number is a binary, it must be. On a piece of paper, you know, human to human, power of 10 would be more useful to elucidate.

Q. So you're not aware of any computer implementations of Montgomery reduction where the radix is not 2?

A. No. As an expert, as a teacher in computer arithmetic, I have seen other values of R being simulated. But the need of implementation is when R is a power of 2.

30

Q. Let's go to paragraph 46, please, on page 15.

A. Okay.

Q. The second-to-last sentence says [as read]:

"One then shift a to the right by one word, thus reducing the length of a."

Do you see that?

A. Yes.

Q. So what is a in this example? Is it a value, a reductant, an operand? What would you call it?

A. It's one of the temporary results starting from reductant, ending up with the deduced value. It would take it one of the temporary values.

Q. So if you look at the Figure 4 pasted into your declaration, which is on the next page --

A. Yes.

Q. -- the temporary value here that you're talking about would be a, including a 9 through zero at the top, correct?

A. Yes.

31

Q. So in this example, a is comprised of ten words, correct?

A. A0 to a9, yes, ten words.

Q. And so the shift causes the length of a to be reduced by one word, correct?

A. Look at the figure very carefully. You will see that, starting with a9 to a0, n times n added to it, which may cause an extra k or c. But, however, also 0 is the least significant word, a0. The new value of the a0, now 0.

So now together, if you count them, it actually -- you didn't reduce it. You, in fact, increase it to 11 words because now you must include c in it.

But when you're shifted to right, that zero disappears but remains as ten words because c is still there.

Q. The c is called a carry, correct?

A. Carry word, yes.

Q. And that's not part of the original -- the original -- can we call it an operand? Is a an operand in this case?

A. C is obtained by adding mn to a. So it continues to be part of a now.

32

Q. So then help me understand here the sentence that we were talking about at the -- near the bottom of paragraph 46.

You said [as read]:

"One then shift a to the right by one word, thus reducing the length of a."

So it says "reducing the length of a," but then you testified that what you're actually doing is making it longer and then bringing it back to the same length. So in what sense is it reducing the length?

A. If you continue to look at Figure 4, you will see, after c is introduced in the next step, a new c is being introduced in the following step, a new c and a 0 being reduced to the left. And the following step, two 0 is introduced. In the following step, three 0s are introduced. You're making the numbers smaller and smaller in this process.

Q. So --

A. So adding mn, adding mn may or may not immediately reduce the number; but in the final step, what you will obtain is a number that's equal to a mod n, a or inverse mod n for

33

Montgomery.

Q. So if I understand you correctly, in the first iteration, the length of a is not reduced. But by the time you do several iterations -- it's after you do several iterations that the length is reduced; is that right?

A. True. If you look at this example after the second iteration, it's reduced one word. After the third iteration, it's reduced two words and moves on that way.

Q. And what is the purpose of making a shorter in this way?

A. You have a purpose, and you want to compute aR inverse mod n, obtain a number that is less than n. That's your algorithm's objective. You want to accomplish it as shown. This algorithm accomplishes it.

Q. Okay. So as a result of getting a smaller number, the length of a is thereby reduced as well?

A. Finally, it would have to be less than n; otherwise, your algorithm did not work.

Q. Well, let me ask my question a little bit differently.

34

So what I understood you to be saying is the purpose is to make the number smaller than n, but the number that you're trying to make smaller than n is represented by these words, correct?

A. The number -- final number smaller than n is your objective. In between all the temporary results, sometimes the size of it could not be reduced, would be reduced later, so it's not a good idea it will always be reduced.

Q. But by the time you get to the end of the multistep process, the number will be reduced and the length of a will also be reduced, correct, the number of words?

A. Yes.

ATTORNEY DESAI: Objection to form.

THE WITNESS: At the final step, number will be reduced. And a reduced number will have the same length as n.

BY ATTORNEY EKLEM:

Q. Let me just try to clarify this a little bit.

So in paragraph 46, the end

35

of -- the end of the second-to-last sentence, it says [as read]:

> **"Thus reducing the length of a."**

So I think there are two concepts here. There's the length of a, and then there's the number you're trying to make smaller than n.

Those are not necessarily equivalent or -- you know, they're not identical concepts, right? They're kind of two different concepts; is that correct?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Number a is a temporary -- the number a in any one of those five steps in Figure 4 is the temporary result whose computation will finally give you a mod n -- aR inverse mod n. That's all there is to it.

BY ATTORNEY EKLEM:

Q. So at the beginning, we said that -- at the top of the example, a comprises ten words, correct?

A. Yes.

36

Q. And at the end of the example, a comprises six words if you count the carry, correct?

A. Correct.

Q. So the reduction process took you from ten words to six words, correct?

A. I didn't hear you. There was a breakup. Can you repeat your question?

Q. Yes.

The reduction process took you from ten words to six words, correct?

A. Correct. In this example, yes.

Q. And the reason why it went from ten words to six words is because the number that the words represent was reduced mod n, correct?

ATTORNEY DESAI: Objection to form.

THE WITNESS: Finally, it would deduce mod n, but the reason that it becomes smaller is because the lower part of it, lower word of it, becomes zero by the additional mn. And then shift it to right would bring you a product factor of R to the minus w, whatever w is. And, eventually, all of these would give you --

37

all of those steps would give you a reduced number, much less.

BY ATTORNEY EKLEM:

Q. So this example shows the Montgomery reduction being performed in multiple steps, and I think the figure labels it Steps 1 through 5, correct?

A. Correct.

Q. Now, the Montgomery reduction technically does not have to be performed in five steps, correct? It could be done in just one?

A. Montgomery reduction, as described here, continues to add mn, where at each Step 1 word becomes zero and the least significant word. So the number of steps is equal to really approximately the number of words.

So that's -- that -- what you end up doing is you add a ten-word number; you end up with that six-word number. So, therefore, you have reduced the five words using five steps. That's approximately what happens.

Q. So you're doing it in multiple steps because you have multiple words that represent

38

a, correct?

A. I'm doing in multiple steps involving the words because that Montgomery algorithm can work that way.

Q. And Montgomery algorithm works that way because some numbers are too big to be represented in a single machine word, right?

A. The objective of Montgomery algorithm to have -- to reduce a number to the finite field, modular n. That's the objective.

Q. Yes. Well, as we discussed before, right, a modulo n operation could be done in one step, right?

Like, your example in paragraph 32, you were explaining how there's two ways to do a modulo. You could do one step, like 375 modulo 97 equals 84, or you could break it up and reduce intermediate -- intermediate results and get the same answer of 84, right?

ATTORNEY DESAI: Objection to form.

THE WITNESS: You're mixing concepts here.

39

BY ATTORNEY EKLEM:

Q. Okay.

A. That example in paragraph 32 has something to do with the -- doing the reductions as the operations, multiplications and additions, are done, interleaving them, a little bit of multiplication and addition and a little bit of a reduction, continuing that way.

And -- or just going ahead and finishing the multiplication and doing reduction later, which would still be multiple steps, as Figure 4 shows us.

Q. Okay. So then going back to paragraph 46.

A. Okay.

Q. I just want to -- I think -- I think I understand what's going on here.

So the sentence we were talking about there, the second-to-last one, the [as read]:

> **"One then shift a to the right by one word, thus reducing the length of a."**

That's the sentence I'm talking about.

40

Do you see it?

A. Yes.

Q. Okay. So what I think -- what I think I understand is that it's not -- it's not just the shifting to the right by one word reduces the length of a, but, instead, it's shifting to the right as many times as it takes to get to the end of your result to achieve aR to the minus 1 mod n, right?

ATTORNEY DESAI: Objection to form.

THE WITNESS: As I explained to you the way Figure 4 works, for example -- not for example.

Just look at Step 1. You have a ten-word a. And Step 2, you still have ten words, because you introduce c even after the shifting before shifting at 11.

And then Step 5, now you have introduced one extra zero; now you have nine words, et cetera.

So, therefore, this algorithm, the way it works, by adding multiples of n, zeroing the least significant word, still the number could be 10 or 11 words.

41

And then shifting it bring it to either nine or ten words -- in this case, ten words.

And continuing that way, each time introducing the k word but still having more zeros on the left. And the final shifts, every single one of the shifts would give you a mod n -- aR inverse mod n.

BY ATTORNEY EKLEM:

Q. When you do Montgomery reduction this way, is there always a carry?

A. Carry is not always. It's a statistical phenomenon. It happens sometimes, and it doesn't happen some other times.

Q. Well, what do you mean by "statistical phenomenon"? Does that mean it happens rarely?

A. Not rarely. It happens with at least or nearly 50 percent chance because you're adding a plus mn. The mn could introduce a carry or could not introduce a carry, and there's a chance of at least 50 percent.

ATTORNEY EKLEM: Okay. I lost track of my time.

Joe, how long have we been on the record, or Jennifer, either of you?

THE VIDEOGRAPHER: Yeah. We have 58 minutes.

ATTORNEY EKLEM: Okay. Let me just do a couple more questions.

And then, Dr. Koc, you want to just take a short break?

THE WITNESS: As you wish.

ATTORNEY EKLEM: Okay. So give me a second here.

Actually, let's just go ahead and do a short break.

Is five minutes okay?

THE WITNESS: Fine.

THE VIDEOGRAPHER: Okay. We are now going off the video record. The time is 9:06 a.m.

- - -

(Whereupon, a short recess was taken.)

- - -

THE VIDEOGRAPHER: We are now going back on the video record. The time is 9:20 a.m.

ATTORNEY EKLEM: Thank you.

BY ATTORNEY EKLEM:

Q. Welcome back, Dr. Koc.

During the break, did you discuss the substance of your testimony with counsel?

A. No.

Q. Okay. Let's go to paragraph 51 of your declaration, please.

A. Yes.

Q. If you want to review it, go ahead. I'll just have a couple of quick questions about this paragraph. Whenever you're ready, just let me know.

A. Go ahead and ask.

Q. Great.

So in paragraph 51, you refer to a step called "cancelation." And my question is:

Is it your opinion that "cancelation" means the same thing as zeroing?

A. Yeah, yes.

Q. Okay. So you say that [as read]:

"'Cancelation' is a term understood in the art of

modular arithmetic of performing an operation that 'zeros' certain words."

Do you see that?

A. Yes.

Q. Okay. And you have a citation here to a document, Exhibit Y.

A. Yeah.

ATTORNEY EKLEM: I'm going to put that up really quick.

Let's see. That's Doc 11?

THE VIDEOGRAPHER: Doc 11. Stand by.

You want to mark it?

ATTORNEY EKLEM: Yes, please.

THE VIDEOGRAPHER: Stand by.

BY ATTORNEY EKLEM:

Q. Dr. Koc, feel free to look at your hard copy instead. Up to you.

A. I have it.

THE VIDEOGRAPHER: Document 11 will be Exhibit 4.

- - -

(Whereupon, Exhibit 4 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. Okay. And just let me know when you have that in front of you.

A. Which page are we talking about now?

I'm ready.

Q. Let's go to -- let me get the -- it will be -- so the excerpt is four pages long. So it's the third and fourth page. Let's start on the fourth page, which is number 96 in the top left, but in the bottom right ends with 3440.

A. Okay.

Q. Do you see, near the bottom, the Section 3.2.2, "Floating-Point Subtraction"?

A. Yes.

Q. What is floating-point subtraction?

A. The first question is what is floating point?

Floating point is a standard for representing real numbers on a computer. So, therefore, the real-number subtraction would be emulated by floating-point numbers being subtracted.

Q. Okay. So then specifically on the

46

top of the next page, which is 97 in the top right or 3441 on the bottom right, the portion -- the very beginning portion of the page carries over from the previous.

And the second line there on this page says [as read]:

"This cancelation can be dramatic."

Do you see that?

A. Yes.

Q. The cancelation that this document is talking about is the result of subtraction, right?

A. Yes.

Q. So how is this the same kind of cancelation that happens when a multiple of the modulus is added to the reductant in the Montgomery reduction? Because you're adding in that context.

A. "Cancelation," as a term in modular arithmetic or any other type of arithmetic, implies performing an operation that zeros certain words. And that's all there is to it with this example.

Q. So in this example, your declaration

47

doesn't point to any other usage of the word "cancelation," correct?

A. In Figure 4 that we have been reviewing, in fact, we zeroed in the lower part of the number.

Q. Okay. Well, let me be -- let me ask the question a little differently.

So other than the patent and other than this -- this Exhibit 4 that we're talking about, which is Exhibit Y to your declaration, other than Exhibit Y to your declaration and other than the patent, do you point to any documents that use the word "cancelation" to refer to zeroing?

A. As an expert, I have seen that word to mean and zeroing part of the number. And I have seen in many places, not just in one.

Q. Okay. And what kind of places have you seen it?

A. Computer arithmetic-related context.

Q. You didn't point to any of those other sources in your declaration, right?

A. I referred to that one as a cancelation, and certain words are zero; then that's sufficient.

48

Q. So this excerpt comes from the larger document.

Do you know if -- if you go up to the very beginning of this Exhibit 4 that we're looking at, not the title page that says "Exhibit Y," but the next one, the second one, this is an article titled "Modern Computer Arithmetic" by Richard Brent and Paul Zimmerman, Version 0.2, correct?

A. Correct.

Q. Have you reviewed the entirety of this document?

A. I have read this document for my computer arithmetic courses and presented parts of it to my students.

Q. Okay. Do you know if anywhere in the rest of that -- of this document, in its complete form, does it discuss Montgomery reduction?

A. I don't remember because that was a course in lower division computer science. Montgomery wasn't included.

I don't remember it now.

ATTORNEY EKLEM: So let's go ahead, Joe, and put in Document 12 as the

49

next exhibit.

- - -

(Whereupon, Exhibit 5 was marked for identification.)

- - -

THE VIDEOGRAPHER: It will be Exhibit 5. Stand by.

ATTORNEY EKLEM: Are we looking at Exhibit 5, Joe?

THE VIDEOGRAPHER: Yes. Correct.

ATTORNEY EKLEM: Okay. Sorry. It's the same cover page, so I wasn't...

BY ATTORNEY EKLEM:

Q. So, Dr. Koc, you can either follow along in the screen share or you can download the whole document.

But does this appear to be the same title and author and version number of "Modern Computer Arithmetic" that we were just discussing in Exhibit 4.

A. Yeah. This is the same as what I have as Exhibit Y, yes. I see that document, which is 190 pages, which I assume we're talking about the same document.

50

Q. Yeah. That's right. So -- but let's go to -- you can follow along or scroll through it yourself. But I want to go to PDF page 56, which is Section 3.2 -- 2.3.2.

So here we have a section that discusses "Montgomery's Multiplication." And it carries over into the next page as well.

A. Yes.

Q. Montgomery multiplication involves Montgomery reduction, right?

A. Yes.

Q. Okay. If you want to just look at this section real quick and let me know if you see a discussion of using the word "canceling" in this area of the paper.

A. Section 2.3.2, which is discussing Montgomery multiplication, has a very theoretical view. It doesn't have any examples. It doesn't have the steps of the algorithm, but for other ways to prove properties of the algorithm and the ranges of the numbers involved, et cetera.

So it doesn't -- and that's why that it doesn't come to a place where lower parts of the numbers being canceled by adding a

51

multiple of the modulus to it.

Q. On page 57, the bottom paragraph there that starts with "For example," does this -- does this not show multiplying a multiple or adding a multiple of the modulus to -- to the input C?

A. In this C is equal to C plus 924N beta, is computed, as we can see the lower part of the number zeroed in. So he actually shows that lower parts of zero because that's how Montgomery is proven. Whether or not he used the English expression "cancelation" is not very important.

Q. Okay. But we agree that he does not use the word "cancelation," right?

A. We agree that it does an operation which zeros the lower part of the number.

Q. Right. But my question is just -- it's specifically does this paragraph or any paragraph around it use the word "cancelation" to describe that?

A. This particular paragraph does the steps of the Montgomery correctly and obtains the number correctly.

Q. And it does not use the word

52

"cancelation," right?

A. As I said, this algorithm is correctly executed in two steps here to show that the lower parts are being zeroed in, which is the same concept. Whether or not he uses a very particular expression for that is not relevant.

Q. I understand you don't believe it's relevant, but it -- I guess I don't see the word "cancelation" in that paragraph.

I'm just asking: Do you see the word "cancelation"?

ATTORNEY DESAI: Objection. It's argumentative. I mean, it's not there. So, I mean, do you need him to confirm it's not there?

Dr. Koc, you can answer.

THE WITNESS: And Brent didn't use the word "cancelation" in this paragraph.

BY ATTORNEY EKLEM:

Q. Okay. But he did use it in the discussion of floating-point subtraction, right?

A. He may have used it in other places

53

too, yeah.

ATTORNEY EKLEM: Joe, let's put in Document 10 as the next exhibit, please.

- - -

(Whereupon, Exhibit 6 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. Dr. Koc, Exhibit T, as in Tom, to your declaration.

A. Okay. I have it.

Q. Great.

So now on the third page of the document, the bottom right corner -- well, the bottom of the page is 519. The Bates number ends with 1275.

At the top of this page, the title is "Modular Multiplication Without Trial Division" by Peter L. Montgomery.

Do you see that?

A. Yes.

Q. So this is the original Montgomery paper, Montgomery reduction paper, right?

A. Yes, it is.

54

Q. This paper does not use the word "cancelation" to describe the process of Montgomery reduction, does it?

A. Montgomery original paper is known to be extremely compact paper. As you can see, it's only three pages -- in fact, two pages, because one of them is references. So, therefore, he was very succinct in trying to make a point that t gets T plus mN divisible by R. That's all he cared.

All he cared was to show people, hey, T plus mN is divisible by R. So that's all he did. And he didn't give an example. He didn't go through the steps.

He's a very succinct person. I have known him and when he was alive and he was living, and we had worked in the same university. Yeah. That's what he does. Very succinctly, he just tries to prove that T plus mN is divisible by R, period.

Q. You can set that aside.

Let's go back to your declaration, paragraph 52, please.

A. Okay. I have it.

Q. Okay. The last sentence of -- on

55

this page carries over to the next page. It's not the last -- it's the second-to-last sentence of the paragraph. And it begins with [as read]:

"It describes this replacement."

Do you see that?

ATTORNEY DESAI: What page was that again? I'm sorry.

ATTORNEY EKLEM: Oh, sorry, Joe. We're on --

THE WITNESS: This is -- I don't have the correct -- yeah.

BY ATTORNEY EKLEM:

Q. That's okay. It's page 19 of the declaration, which is Exhibit 1 to the deposition.

So, again, Dr. Koc, it's paragraph 52 of your declaration on page 19.

THE VIDEOGRAPHER: Got it.

THE WITNESS: Yeah.

BY ATTORNEY EKLEM:

Q. Yeah, so at the bottom of the page is a sentence that begins with -- it describes this replacement, and that sentence carries

56

over to the next page. I just want to point that out because you need to look at the whole sentence here.

A. Yeah. I do. I see it.

Q. So in that sentence, you say that [as read]:

"The term a0 times n prime times 2 to the w is necessarily modularly equivalent to a0 mod n."

Do you see that?

A. Yeah.

Q. Why is that term necessarily equivalent to a0 mod n?

A. The way n prime is computed.

Q. So the modular equivalence comes from the way n prime is computed?

A. Yes.

Q. And n prime is computed -- I think you have it a little higher up in your paragraph. There's a sentence that says [as read]:

"Specifically, the '286 Patent describes using the 'new value' n prime equals

57

2 to the minus w mod n for performing Montgomery reduction."

Do you see that?

A. Yes, it does.

Q. Okay. So that's what you're referring to, the computation of n prime where it equals 2 to the minus w mod n?

A. Yes. In fact, 2 to the minus w n times 2 to the w together would give you one modular n. That gives you a0. So a0 is equal to a0 mod n.

Q. So the multiplying by 2 to the minus w is necessary here to make it equivalent to a0 mod n, right?

A. Multiplying by 2 to the w, together a0 n prime, would necessarily give you a0 equal to a0 mod n.

Q. Okay. So then if I took out the 2 to the -- if I took out 2 to the w and if -- if it would -- suppose it was just a0 times n prime; is that still modularly equivalent to a0 mod n?

A. When you're multiplying a0, it would be -- when you're multiplying a0 by another number and adding it to the rest of the a, but

58

multiplying a0 by another number, you would obtain a number not necessarily equal to mod n.

Q. Okay. So multiplying 2 to the w -- yeah. So let me -- let me start over here.

So in the expression a0 times n prime times 2 to the w, that expression needs to have 2 to the w there for it to be modularly equivalent to a0 mod n, right?

A. Yes.

Q. Okay. I see.

Okay. My notes are -- let's go to paragraph 55, please, on page 21.

In the middle -- right about in the middle of the paragraph there's a sentence that begins about -- you know, it begins with [as read]:

"Because the LSW of the addend a0 times n prime times 2 to the w."

Do you see that sentence?

A. Yes.

Q. Okay. That sentence -- inside that sentence there's parentheses, and it says [as read]:

"Multiplying 2 to the w

59

adds w number of zeros to the end of the addend."

Do you see that?

A. Yeah.

Q. So how does multiplying 2 to the w add zeros to the addend? Because I understand how it works in the decimal example that you gave where you're using ten, so that makes -- that's intuitive.

But in this context, where it's multiplying by 2 to the w, how does that create zeros?

A. Whether it's modular 10 or modular 2 doesn't really makes difference except that humans understand modular 10 better.

'286 Patent offers a modification to Montgomery algorithm by introducing n prime, which is equal to 2 to the minus w mod n.

And the example on page 23 of my declaration shows the steps of it, where you can either zero LSW of the reductant or don't. And if you add a0 n prime 10 to the w to it, you would have the least significant digit, zero. And that is what the premise of the

60

patent is. And this example closely follows it.

Q. So in the answer you just gave, you said -- you said you can either zero the least significant word of the reductant or don't.

So you were describing the patent, right? You're saying the patent teaches that you can -- hold on.

So you're saying that the '286 Patent teaches that you can either zero the least significant word of the reductant or don't?

A. No, that's not what I said.

'286 Patent gives one embodiment, which I have shown in this particular -- in paragraph -- the example in paragraph 56.

And there, to your question, as highlighted in yellow here, equals the LSW of the addend is also zero.

The answer, yes, it would be zero, because 2 to the w multiplied by 2 to the w, any number, would introduce w 0s to the right of it in bits.

And multiplying any number by 10

61

to the w in my example would introduce w0s in decimal to the right of it. And this is the embodiment given in the patent.

However, it can be shown that you can 0 the LSW and add the addend. Or you can add 0 or not. You can add not n prime, not a0 n prime 2 to the w, but a0 n prime plus n times 2 to the w or minus n 2 to the w. All of those would also work.

And that's the statements in my declaration source very clearly. But when I look at the patent, I see only one of them being shown by example.

And the other one in part of the patent was mentioned in the specification part just in passing. It could be negative also, which means the patentor was aware of it probably.

Q. Okay. So then let's go to paragraph 57 of your declaration, please, on page 23.

A. Yeah. Right here.

Q. So the first sentence here says [as read]:

"While both standard

62

Montgomery method and the '286 Patent's method involve clearing the least significant portions of an unreduced operand and leaving the remainder in the more significant portions, each does so in mathematically distinct ways."

Do you see that?

A. Yes.

Q. So what do you mean by "clearing" in this sentence?

A. Cancelation. Making 0.

Q. So let's move on to paragraph 73 of your declaration, please.

Yes. 73, which is --

A. Yes, I have it.

Q. -- bottom of page 30.

A. Yes. I have it.

Q. This is talking about -- this is in the context of different patents, right? This is not the '286 anymore.

A. Yeah.

Q. Actually, the exhibit to your

63

declaration that you're citing here is the '062 Patent. So I just want to set that straight.

So paragraph 73 here, you're discussing portions of the '062 Patent, correct?

A. Yeah.

Q. Okay.

A. I think that's correct.

Q. All right. So in paragraph 73, the second sentence -- I'm sorry -- the first sentence says [as read]:

"The specification describes two types of reduction: one that is 'specific to a certain finite field, or a wordsize reduction.'"

Do you see that?

A. Yes.

Q. So in that sentence of the '062 Patent, it's your opinion that the '062 Patent is referring to two different types of finite field reduction?

A. Two types of reduction. One is to

64

the finite field, and the other is wordsize reduction.

Q. So the wordsize reduction is not a finite field reduction, correct?

A. Wordsize reduction allows you to eventually do finite field reduction if that's your objective.

Q. But the wordsize reduction is not itself a finite field reduction, right?

A. Again, it depends on the context. If it is very clearly some algorithm like Montgomery is being used, which keeps the number modular n along its computations and then, therefore, wordsize reduction would eventually produce a number that is equivalent to a number inside the finite field.

The difference between finite field reduction was the word size in this context as was given in the specification of this patent. And the finite field reduction, you would have the number reduced less than n.

And the wordsize reduction, you would just -- it's okay to keep the number larger than n but still within certain number of words so that the registers keeping the

65

number would not be overflow. That's their difference.

Q. So you said in the wordsize reduction it's okay to keep the number larger than n?

A. In paragraph 74, I explain that further.

Q. Okay. I saw that you gave an example of how that could work in paragraph 74, but does the patent say that?

A. As an expert with the wordsize reduction and finite field reduction, this is my understanding of what each one of them is. In paragraph 73 and 74, I try to explain that.

Q. Okay. I just -- I mean, we can look at paragraph 74 here for a second. I just want to make sure that I didn't miss something.

I understand it's your expert opinion that with wordsize reduction the number can stay larger than n. But does the patent itself say anywhere that in the wordsize reduction the number can stay larger than n?

A. The patent says that the wordsize reduction should lower the length of the result to appropriate word length of the underlying finite field so that those numbers can be kept

66

in registers of the same word length. And my paragraph just explains that.

Q. Okay. Well, we'll get to that example here in a second.

Actually, let's just go to paragraph 74 here for a minute.

So in paragraph 74 -- in paragraph 74, you're describing the wordsize reduction or what you're calling the wordsize reduction, correct?

A. Yes. In 73, I'm describing reduction with respect to a finite field. In paragraph 74, I describe wordsize reduction.

Q. Okay. When you're describing the wordsize reduction in paragraph 74, you have a citation in the middle of your paragraph to Column 8, lines 44 through 47, of the '062 Patent.

Do you see that?

A. Yeah, I do.

Q. Okay. So let's take a look at that real quick.

ATTORNEY EKLEM: Joe, that's Document 6. Let's enter that as the next exhibit.

67

- - -

(Whereupon, Exhibit 7 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. And, Dr. Koc, I believe that's Exhibit D to your --

A. Yeah. Okay.

Q. -- to your declaration, if you have your copy of it.

A. I do.

THE VIDEOGRAPHER: I'm marking Document 6 as Exhibit 7.

THE WITNESS: Go to Column 8?

BY ATTORNEY EKLEM:

Q. Yes, please. Yeah. Let's go to Column 8. And then let's just focus on the lines 40 through 49. That should be enough.

THE VIDEOGRAPHER: What page is that? I'm sorry.

ATTORNEY EKLEM: It's in Column 8, so I don't have the page number. But just keep going down. I'll tell you when to stop. You'll start seeing the columns there in a second.

68

THE WITNESS: Okay.

BY ATTORNEY EKLEM:

Q. And then lines 40 through 49 --

A. Yeah.

Q. -- I just want to parse this out a little bit.

So at the end of line 40, there's a sentence that says [as read]:

"After applying the wordsized algorithm 440, the finite field engine reduces the result using a finite field reduction 450."

Do you see that?

A. Yes.

Q. Okay. So -- so the first thing here is this finite field reduction 450. And then the next sentence says [as read]:

"The finite field reduction may be specific to a certain finite field, or a wordsize reduction."

A. Yes.

Q. So that sentence is describing something about the finite field reduction 450, right?

69

A. Yes.

Q. Okay. And then the next sentence says [as read]:

"The reduction should lower the length of the result to the appropriate word length of the underlying field."

Do you see that?

A. Yes.

Q. Okay. So when it says "the reduction," is it your opinion that the reduction in that third sentence is only talking about the wordsize reduction and not talking about the specific reduction?

A. The following sentence gives you the clue. The following sentence says [as read]:

"This way the finite field elements may be consistently stored in registers of the same word length."

So they're talking about wordsize reduction.

Q. Do you think there's another way to

70

interpret that where the reduction that lowers the length of the result is what is supposed to be accomplished by the finite field reduction 450?

A. The finite field reduction is supposed to obtain a number that's less than n if you're talking about modular n prime fields.

And then the wordsize reduction produces a number that fits to the available word length, not beyond that.

Could still be less than n. Could be larger than n. There's nothing confusing here, neither in the patent nor in my paragraphs, two paragraphs. It's very clear.

Q. Could a reduction specific to a certain finite field achieve the purpose of lowering the length of the result to the appropriate word length of the underlying field?

A. We have discussed this before. If the given input is already -- after, let's say, a multiplication, it's already less than n, we end up not reducing it further.

So reduction in length is not given, not always -- not always happens. But

71

it has to be less than n. That's all there is to it.

Q. Right. But my question maybe was just a little bit different.

My question is:

Could -- is it possible for a reduction specific to a certain finite field to achieve the purpose of lowering the length of the result to the appropriate word length of the underlying field?

A. I have given several examples in this paragraphs and the follow-up paragraphs that the reduction in total length may not necessarily happen at all times.

Q. So --

A. In the following paragraph, 76, I give very specific examples.

Q. Right. So your examples, I think you said, are intended to show that the -- that it may not necessarily lower the word length, but it could, right?

A. Yeah. That necessarily means that. "Not necessarily" means exactly that it could. It may not.

Q. Okay. So in paragraph 74 -- I just

72

want to get a quick clarification of something here.

The last sentence of paragraph 74 before -- before your bullet point examples, it says [as read]:

"The patents teach storing a" --

Excuse me. It says [as read]:

"The patents teach storing a finite field elements in two words because the modulus," and then it gives parentheses.

It's a little unclear to me what you mean here. It says "because the modulus."

But "because the modulus," what?

A. In the previous sentence, it says [as read]:

"A system of having word size of 3 and a finite field modulus of 10,007."

And then -- so two words because 5 over 3 rounded up is 2. And so, therefore, all the numbers are -- in this particular finite field, will have two words.

73

And so a number like 10 million reduced to the specific finite field of 10,007 becomes 3,007. But if you do a wordsize reduction of 10 million, then you generate a two-word number congruent to the same number, same result, 3,007.

For example, you would have -- 993,700 would be an acceptable result because they are congruent and they take six digits or two words.

Q. Okay. So --

A. I explain it that way. And there's nothing wrong here in this part.

Q. So then let me just make sure I understand.

When you say, "The patents teach storing a finite field elements in two words because the modulus," that means that it teaches storing the elements in two words because the modulus -- it's a function of the size of the modulus, right?

A. Yeah. Modulus size.

Q. Okay. So in that sentence, it's specific to the modulus?

A. Yes, of course. Everything we do is

74

specific to the modulus. We're doing finite field arithmetic in prime fields. We have a particular modulus, in this case 10,007, which requires six digits or two words. One word has two digits.

Q. Okay. So the modulus is a characteristic of the finite field that you're working with.

A. The modulus defines the finite field.

Q. Okay. So the wordsize reduction reduces the length to a size that is specific to the modulus of the finite field, right?

A. No. Wordsize reduction reduces a number specific to the number of words selected for that operations.

That's why you have 993,700, not a number less than 10,007.

Q. And is the number of words selected based on the modulus of the finite field?

A. Precisely. It could be, as long as it's not less than that. It can be bigger if 10,007 is five digits. You could at least select six digits, or you could select eight digits, ten digits, all fine.

Q. So the wordsize reduction is specific to the finite field that you're working with because it's based on the modulus, right?

75

A. No. Wordsize reduction is aspecific to the number of words the numbers are represented. And the reduced number could be larger than the modulus but less than the number of words --

Q. Okay.

A. -- it's the total the number of words.

Q. The number of words that you choose to use is based on the modulus that you're working with, right?

A. It cannot be less than modulus, but it has to be bigger than the modulus. And it can be quite big, like in this case.

Q. So you have two bullet points that are two different examples in paragraph 74. Let's talk about the first one for a second.

A. Yeah.

Q. The words here say [as read]:

> **"Reducing 10 million with the specific finite field: 10 million mod 10,007 equals 3,007."**

76

Do you see that?

A. Yes.

Q. So what do you mean by "reducing with the specific finite field"? Because that sounds different than reducing -- okay. So let me just take a step back.

So the part of the patent that we were talking about discussed these, you know, what we say are two types of reduction. One of them was a reduction specific to a certain finite field, and here you're saying it's a reduction with the specific finite field.

Is there a difference there?

A. Two.

Q. So why is the first example here -- in what way is it specific to a finite field?

A. The finite field modulus is n equals to 10,007, the result is less than 10,007:

That's why.

Q. Okay. It's specific to the finite field because of the fact that you're using a specific modulus, right?

A. Modulus defines the finite field. For the same finite field, I cannot use a different modulus. It has to be -- there's only one modulus for every finite field.

77

Q. Okay. So in your second example, you call it wordsize reduction. And it says [as read]:

> **"Generate a 6-digit (2-word) number congruent to 3,007 mod 10,007, for example, 993,700."**

Do you see that?

A. Yes.

Q. Okay. So why are you starting with 3,007?

A. Because that's what the result must be congruent to.

Q. And it must be congruent to that because 10 million mod 10,007 is 3,007, right?

A. Indeed.

Q. So in your second example, the number you're generating depends on the modulus, correct?

A. All numbers -- all numbers generated temporarily or finally must be congruent to one another modular n.

Q. Okay. So this wordsize reduction is

78

specific to this modulus, 10,007, right?

ATTORNEY DESAI: Objection to form.

THE WITNESS: It's specific to its size, then it is -- as you can see, the -- we start with 10 million, which is an eight-digit number. They apply the reduction algorithm. If you're lazy, a reduction algorithm would be just continually subtract 10,007 from 10 million.

Keep doing it until you obtain a number that's in six digits; you can stop. That is the number 9,900 rather than 3,700, which is equal to 3,007 modular n, n being 10,007.

BY ATTORNEY EKLEM:

Q. So in the first example, the result of the modular operation is 3,007, correct?

A. Yes.

Q. So that -- that fits into two words, correct?

A. That 10,007 doesn't. 10,007 requires six words. So any other number could be as big as -- nearly as big as 10,007.

79

For example, any result like 10,006 would require five digits, which is at least two words, which is actually six digits.

Q. Well, so in your second example, you're seeking to generate a six-digit, two-word number, correct?

A. My goal is to end up with a six-digit number, not more.

Q. Okay. But by doing the procedure in the first example, 10 million mod 10,007, you get a number that fits within two words, right?

A. It does. But any other number -- 20 million may not produce a four-digit number. You know, two-digit number. Two-word number, you know. Another number, another number, another number. You need to make sure that you have a space for all possible outputs which are as big as 10,007, which is five decimal digits and two words. And we have decided that we want to give them six digits -- decimal digits because two words actually allows you six decimal digits.

So just because one example is only two digits, another example could be even one digit. Would you reserve a one-digit space

80

for all such numbers? That would be very incorrect.

Q. Well, I guess what I'm trying to get to is in your second example -- so both examples are performing some kind of reduction on 10 million, right?

A. Yes.

Q. And the second example creates a six-digit, two-word number by finding one that is congruent to 3,007 mod, 10,007, right?

A. Correct.

Q. So if you -- so you're looking for -- you're looking for -- you're looking for a number that's congruent to something that you've already determined.

A. No, that's not correct. I don't know what I am producing with the reduction algorithm. The reduction algorithm keeps working. We have -- together we have looked at Montgomery as well as '286. That algorithm continually work on the number step by step. And here in bullet number 2, the reduction algorithm is instructed to stop when a six-digit number is reached. Stop. And stop, what did they get? 993,700. Perfect.

81

Is this number mathematically equivalent to 3,007 modular n? Yes. But the computer didn't know that algorithm, doesn't know that algorithm. Just reduce it with respect to the modulus.

It doesn't compute part of them and then, oh, compare them. We don't do it that way. We just have a reduction involved, reduction of Type 1, reduction of Type 2. One is specific to a finite field reduction, modular n. The other one is with respect to the wordsize reduction, which is six digits or four words, two words here.

Q. So in the -- in the section of Column 8 that we were discussing in the '062 Patent, it says [as read]:

"The reduction should lower the length of the result to the appropriate word length of the underlying field."

Right?

A. Yes, it did. In fact, it's still open in front of me, you know, that --

Q. Yeah.

A. -- Column 8, yeah.

Q. Yeah.

So if your goal is to get it down in your example to two words, six digits or two words, that can be achieved by just doing the first example, right?

A. Finite field reduction will also end up a number that is less than six digits. And wordsize reduction, when it reaches six digits, it stops.

Q. So why not just take 3,007 and put two zeros in front of it? Then you have six digits and two words.

A. 3,007, two zeros in the left or right?

Q. On the left. 003,007.

A. Where did you get the number?

Q. Well, let's look at -- let's go back to the '062 Patent, Column 8.

A. Okay.

Q. I'm sorry here. Hold on one sec.

Yeah. Column 8, line 30 to 35.

A. Okay. I'm here.

Q. So the second sentence -- well, actually, the whole thing here. Let's start with the first one.

[As read]:

"Finite field elements are stored by the finite field engine and memory segments larger than are actually required. The most significant bits are set to 0. Operations can be performed on these elements by acting on the memory segment as a whole, while ignoring the extra digits. This representation is referred to as 'wordsized' representation."

So why couldn't you just do that, take 3,007 and add zeros to the significant side to make it match what you're trying to do?

A. Can we go back to my declaration, to that 74 paragraph?

Q. Yes.

THE VIDEOGRAPHER: I apologize. I didn't hear that. You said "declaration"?

THE WITNESS: Yes. Declaration,

paragraph 74.

THE VIDEOGRAPHER: Stand by.

THE WITNESS: Here we have two inputs to the reduction algorithm. Two inputs: 10 million and 10,007.

We don't know what the output is. Output is being computed by the reduction algorithm.

The reduction algorithm computes the output, 3,007. It could have been some other number. You're welcome. So 3,007 is that.

In fact, when it is computed, it already had two zeros in front of it because it's in a register of six digits. Already had that two zeros.

You cannot -- 3,007 is not given to you. You compute that.

I hope I am clear.

BY ATTORNEY EKLEM:

Q. I think so.

So if the zeros are already there with 3,007, then it doesn't -- so then doing example one has the effect of the wordsize reduction of ensuring that it fits

within the required number of words, right?

A. N is already less than the number of words provided. When it's less than n, it would be less than the number of words n resides in.

ATTORNEY EKLEM: I think we've been on for a little more than an hour, Dr. Koc.

Would you like to take five minutes?

THE WITNESS: Sure.

THE VIDEOGRAPHER: Okay. We are now going off the video record. The time is 10:31 a.m.

- - -

(Whereupon, a short recess was taken.)

- - -

THE VIDEOGRAPHER: We're now going back on the video record. The time is 10:40 a.m.

ATTORNEY EKLEM: Thank you.

BY ATTORNEY EKLEM:

Q. Dr. Koc, during the break, did you discuss the substance of your testimony with

86

counsel?

A. No.

Q. Okay. So let's go to paragraph 80 of your declaration, please, on page 33.

A. Yeah. I have it.

Q. So in paragraph 80, just to be clear, you're citing some portions of the '370 Patent, so we'll be talking about a different patent here.

In paragraph 80, you say [as read]:

> **"The specification states that 'omitting the public key from the certificate can save on bandwidth and storage and the verification process described above yields reduced verification times.'"**

Do you see that?

A. Yes.

Q. Do you have an understanding of what bandwidth is?

A. Of course.

Q. Could you explain?

A. At the speed at which data can be

87

delivered.

Q. Okay. And, I mean, is it common to measure bandwidth in units of bits per second or megabits per second or gigabits per second, et cetera?

A. Yes.

Q. Okay. So the more data that needs to be transmitted, the more time it takes to transmit it, right?

A. True.

Q. So you could -- you could analyze the amount of time it takes to transmit data or, rather, the time it takes -- hold on. Let me start over.

Actually, strike that. That's okay.

Shifting over to paragraph 81.

A. Okay.

Q. In this paragraph, you cite a few -- three different portions of the '370 Patent.

Do you see that?

A. Yes.

Q. Okay. One of them is Column 9, lines 9 through 15.

ATTORNEY EKLEM: So, Joe, that's

88

Document 8. Let's go ahead and enter that.

- - -

(Whereupon, Exhibit 8 was marked for identification.)

- - -

BY ATTORNEY EKLEM:

Q. And, Dr. Koc, that's Exhibit F.

A. Yes.

Q. F, as in foxtrot, to your declaration.

A. Are you going to put it on the screen or not?

ATTORNEY EKLEM: Did you catch that?

THE VIDEOGRAPHER: Stand by. It's laggy. It should come up in a minute.

And we're going to mark Document 8 as Exhibit 8.

ATTORNEY EKLEM: And then if you want to take us to Column 9, Joe, lines 9 through 14. Yep. That paragraph.

THE WITNESS: Yeah.

89

BY ATTORNEY EKLEM:

Q. So, Dr. Koc, do you see, in the last sentence there, it says --

A. Yeah, I do.

Q. -- [as read]:

> **"In other words, 33 percent more signatures can be verified in a given amount of time using the embodiment described above"?**

Do you see that?

A. Yes.

Q. Okay. So what it's considering here is a number of signatures verified per amount of time, correct?

A. Yes.

Q. All right. Let's go to paragraph 83 of your declaration, please.

A. 83?

Q. Yes.

A. Okay.

Q. And so this -- we're shifting now. This is in the context of the '961 Patent, "Random Number Generators" section of your report.

90

A. Yes.

Q. So different patent. I just want to level set.

So in paragraph 83 --

A. Yeah.

Q. -- you distinguish between random number generator, RNG, and pseudorandom generator, PRNG, correct?

A. Correct.

Q. Okay. And in paragraph 84, the next paragraph, you say [as read]:

"To achieve true randomness, RNGs rely on 'naturally occurring' source of randomness, not deterministic functions or algorithms."

And the next sentence says [as read]:

"'Physically' or 'naturally occurring' sources of randomness may include any form of physical entropy, such as thermal noise, atmospheric noise, radioactive decay,

91

recorded audio or video feeds, or even mouse movements on a computer over time."

Do you see that?

A. Yes.

Q. Okay. So the RNGs that you're referring to in your report, as distinct from PRNGs, the RNGs achieve true randomness using physical or naturally occurring sources of randomness, right?

A. I should probably give you an overview of the subject, then it becomes better understood.

The subject of random numbers, random number generator has been in flux since 1990s.

And by around 2000 or so, it has been well established because cryptography has matured. And we understood what kind of randomness we need in cryptography versus in other fields where randomness could -- are used. For example, printing lottery tickets or performing physical simulations, et cetera.

RNG is really a general name. It includes everything. But RNG for

92

cryptography is very specific. And that specifically comes from physically or naturally occurring source of randomness that has higher entropy included.

So PRNGs, without any physical randomness injected, would not be suitable for cryptography.

RNGs, as long as the definition is very clear, if you're in the context of the cryptography, RNGs must include physical entropy and, therefore, useful because we believe that -- as field people, cryptographic engineers like myself, we believe that random numbers should have two properties for cryptography.

One is they have to be uniformly distributed over the values of the numbers; two, they have to be unpredictable. PRNGs do not produce unpredictable sequences of numbers.

They're mathematically related to one another. So, therefore, PRNGs are not suitable.

So now what we do, we don't say "RNG" anymore. We just say "TRNG," true random number generators. But over the past

93

references of books, papers, still use "RNG." And there we should always say, "What is the context?" If its context is crypto, then it is TRNG.

That's my teaching.

Q. Okay. So in your declaration, when you say "RNG," you're referring specifically to the true random number generators, right?

A. Especially -- yes, I do, especially if the context is cryptography.

Q. Okay. And it's your opinion that -- okay.

So with that understanding, it's your opinion that -- so -- so what you're communicating here in paragraphs 83 and 84 is that a PRNG is not an RNG, meaning a PRNG is not a true random number generator, right?

A. The second part of the sentence is correct. That is, PRNG is not a true random number generator. But if you use the word "RNG" for the whole family, PRNG is under the same tree but on the right-hand side, on the left-hand side, whatever, where TRNG isn't.

Q. Have you ever heard of a deterministic random number generator, or DRNG?

94

A. We use the word "DRNG" as a synonym to PRNG.

Q. Okay. And then let's go to paragraph 87 really quick. 87, page 37.

A. Yes. I got it.

Q. The last sentence here of paragraph 87, you say that [as read]:

> **"Depending on the specific security requirements of a given application, this hybrid model, in which a PRNG generates random numbers using a high-entropy seed value, may be referred to as an 'RNG' or 'cryptographically secure PRNG,' because the seed is chosen using a nondeterministic method."**

Do you see that?

A. Yes.

Q. So earlier you said that under the tree of RNGs, one branch is PRNGs, correct?

A. PRNG and DRNG together, yes.

Q. And so a "cryptographically secure PRNG" would be under the -- under that category

95

of -- maybe a subcategory of PRNG/DRNG, correct?

A. Yeah. That's why you call them hybrids, yes, because you borrow from physical source of randomness to enhance the randomness of the PRNGs.

Q. Okay.

ATTORNEY EKLEM: Okay. Joe, let's put in Document 13, please, as the next exhibit.

- - -

(Whereupon, Exhibit 9 was marked for identification.)

- - -

THE VIDEOGRAPHER: Document 13 will be Exhibit 9.

BY ATTORNEY EKLEM:

Q. Do you recognize what's being shown here as Exhibit 9, Dr. Koc?

A. Yes, I do.

Q. Is this one of your textbooks?

A. It is.

Q. And the title is "Cryptographic Engineering," right?

A. Right.

96

Q. Okay. And this is one of the books that was -- that is listed in your CV, right?

A. Yes.

Q. Okay. Let's go to the 23rd page of the PDF.

I think we have a number problem here. Go down one more page, please.

A. That's correct.

Q. So this is page -- numbered page 5 of the book.

A. Yeah.

Q. So the first paragraph under the heading "2.1 Introduction."

A. Okay.

Q. And this is in Chapter 2, the title of Chapter 2 on this page. It says [as read]:

> **"Random Number Generators for Cryptographic Applications."**

Do you see that?

A. Yes.

Q. Okay. And so the first paragraph under Section 2.1 says [as read]:

> **"A large number of cryptographic applications**

97

> **require random numbers, e.g., as session keys, signature parameters, ephemeral keys (DSA, ECDSA), challenges or in zero-knowledge protocols. For this reason, random number generators (RNGs) are part of many IT-security products."**

Do you see that?

A. Yes.

Q. Okay. So in this paragraph, does random number generator, RNGs, refer only to true random number generators?

A. Again, the general name, like I said, RNG sometimes used to mean everything. And for cryptography, it has to be true, or a deterministic random number generator using physical entropy can also pass, depending on the application.

Q. Okay. In the second paragraph of the page, the second-to-last sentence says [as read]:

> **"Ideally, random numbers should be."**

Do you see that?

Page 98

A. Yes.

Q. Okay. Let me read a section of this so I can ask you a question. It says [as read]:

"Ideally, random number generators should be uniformly distributed on their range and independent. However, this characterizes an ideal RNG, which is a mathematical construction.

"In Section 2.2 we formulate the general requirements RNGs should have, and in Section 2.3 we divide the entity of 'real-world' RNGs into several classes."

Do you see that?

A. Yes.

Q. Okay. So this portion of your textbook is distinguishing between an ideal RNG and a real-world RNG, correct?

A. Yeah, it does.

Q. Okay. And so it also describes here two main classes of real-world RNGs called

Page 99

deterministic RNGs and true RNGs, correct?

A. Yes.

Q. So there's at least two kind of RNGs, namely, deterministic RNGs and true RNGs, right?

A. If you look at this section very carefully, an application domain has not been specified. For a general-purpose usage of RNGs, yes, you can definitely say that.

ATTORNEY EKLEM: Okay. Let's go down two more pages to numbered page 7.

Yeah. There we go.

BY ATTORNEY EKLEM:

Q. So on page 7, you see -- so we're still in -- at the top, we have reminders here. We're in Chapter 2, "Random Number Generators for Cryptographic Applications." And now we're in "Section 2.3 Classification.

Do you see that?

A. Yes.

Q. Okay. The paragraph under Section 2.3 says [as read]:

"Following [1] (which narrows the focus to random bit generators) 'real-world'

Page 100

RNGs fall into two main classes. The first class consists of the deterministic RNGs (DRNGs, aka pseudorandom number generators). Starting with a seed, DRNGs generate pseudorandom numbers algorithmically. The true RNGs (TRNGs) form the second class, which falls into two subclasses: physical TRNGs (PTRNGs) and nonphysical TRNGs (NPTRNGs)."

Do you see that?

A. Yes.

Q. Okay. So I think you've said this -- or alluded to this before: Deterministic RNGs is another name for pseudorandom number generators, right?

A. True.

Q. Okay. And whichever way you refer to it, DRNGs or PRNGs, they are a type of RNG, correct?

A. They are.

Q. And true RNGs are another type of

Page 101

RNG, correct?

A. Also true.

Q. Okay. So then just -- you can already see it there on the screen here. Below that paragraph is labeled "Figure 2.1 RNG Classification," showing a tree structure.

Do you see that?

A. Yeah.

Q. So at the top of the tree is RNG, right?

A. Yeah.

Q. So one type of RNG is deterministic, and another type is true or nondeterministic, right?

A. Right.

Q. Okay. And this particular Figure 2.1 says "deterministic" under RNG.

But that's just another way of saying "pseudorandom number generator," right?

A. Well, you repeat it, yes.

Q. Okay. So let's go down to the next page, please, at the top. It's Figure 2.2. The title of it is [as read]:

"Pure DRNG: Generic design."

Do you see that?

A. Yeah.

Q. And it shows the output -- it describes the output of the generic pure DRNG design as a random number.

Do you see that?

A. Yeah.

Q. So at least this textbook considers the output of a DRNG, refers to it as a random number, right?

A. You have to qualify that. You have to go and read the bottom text. You will see that, first of all, as I said, random number is application domain-dependent. If your subject is cryptography, then you want to either use true random number generator or come close to true random number generator as much as possible in order to remain secure.

That's in the previous page. It says [as read]:

"Depending on the 'security anchor.'"

So if you look at this, if you read the bottom, which is the part before the second equation, you'll see that this can --

can this be used for cryptographic purposes? Only if, only if the seed is selected from a true random number generator and that's not sufficient, that functions that you see there, psi and phi, has to satisfy certain mathematical properties in order for that to be unpredictable.

Random numbers for other -- for output applications than cryptography do not need to be unpredictable. They need to be as close to ideal -- ideality, that is, uniform distribution, as possible.

But for cryptography, not only do they have to be uniformly distributed, but they also have to be unpredictable.

To inject unpredictability into this picture, you must select a seed from a physical entropy source and plus you have to select those two functions, phi and psi, very carefully.

Q. So three pages down, on page 11 of the document, yeah, the first full paragraph there that starts with [as read]:

"A class of DRNGs."

Do you see that?

A. Yes.

Q. It says [as read]:

"A class of DRNGs which is very interesting from a theoretical point of view are cryptographically secure RNGs."

Do you see that?

A. Yes.

Q. So cryptographically secure RNGs is a type of RNG, right?

A. Yes.

Q. And in this case, it's a class of DRNG, which is a pseudorandom number generator, right?

A. A class, however, very special because they depend on well-known functions of computability problems.

ATTORNEY EKLEM: Okay. Let's go back four pages -- I'm sorry -- five pages, PDF 24. Yeah, starts with -- nope. Nope. Down one.

Thank you.

BY ATTORNEY EKLEM:

Q. So the second paragraph under

Section 2.2 here says [as read]:

"A closer look at typical applications allows a positive formulation of necessary requirements. Absolutely inevitable is

"(R1) The random numbers should have good statistical properties."

Do you see that?

A. Yes.

Q. So this requirement, R1, is presented as a requirement for RNGs, correct?

A. General-purpose RNGs.

Q. But it has to be true for TRNGs as well, right?

A. TRNGs do also satisfy R1 and more.

Q. Okay. So PRNGs or DRNGs, whichever, and TRNGs have to satisfy R1, correct?

A. Yes. They both do.

Q. Later down on the page is R2.

Do you see that near the bottom?

A. Yes, yes.

Q. R2 says [as read]:

"The knowledge of

106

subsequences of random numbers shall not allow one to practically compute predecessors or successors or to guess the numbers with nonnegligibly larger probability than without knowledge of these subsequences."

Do you see that?

A. Yes.

Q. This is a requirement for DRNGs, TRNGs, and PRNGs, correct?

A. No. This is a requirement for TRNGs. DRNGs or PRNGs do not have this property, not a requirement for them either.

Q. So R2 is not a requirement for PRNGs or DRNGs?

A. That's an incorrect way of stating it. PRNGs and DRNGs do not satisfy art. They only satisfy R1.

TRNGs, on the other hand, satisfy both R1 and R2.

Q. So you're saying that a DRNG or a PRNG does not satisfy R2?

107

A. They don't have to. And, generally, they don't. Yes.

Q. Well, so this section of the book, though, is presenting R1 and R2 as requirements of RNGs generally, right?

A. Like I said, but then it goes into the specifics and says that RNGs for the purposes of general computations, PRNG and TRNG are sufficient to where R1 is satisfied.

But RNGs for the purpose of cryptography must require R2 -- must satisfy R2. And then they can be used for that purpose.

If you want to take a DRNG and use it in cryptography, then you must make sure that you provide some physical entropy to it. Then it comes -- not exactly becomes TRNG but it comes near to it.

That's an expert opinion, not just mine, including this fellow Werner Schindler, who works for German NSA.

Q. So does this -- does this discussion say that DRNGs and PRNGs do not satisfy R2?

I don't see where it says that.

A. Again, you are convoluting the

108

sentence. This discussion says that DRNGs must satisfy R1 and stop there. And TRNGs must satisfy both, R1 and R2.

Q. So the sentence below R2 says [as read]:

"In Section 2.4 we will introduce two further requirements that are characteristic for DRNGs."

Do you see that?

A. Yeah.

Q. So why is it that -- why is it that DRNGs don't satisfy R2 if the further requirements are explained down below?

A. Let's go to 2.4.

Q. Well, my question is about this section, though, because what it's saying is that "further requirements for DRNGs."

A. And just because that sentence is below R2, that you think that it has to be R2. No, it doesn't. So to clarify that, you should go to Section 2.4 to discover what those requirements are.

Q. So you're saying that with a PRNG or DRNG they do allow someone to practically

109

compute predecessors and successors?

A. They are mathematically possible. And many -- there are many examples of cryptographic systems broken because those computations were possible.

Q. So "practically compute" means "possible to compute"?

A. More than that.

ATTORNEY DESAI: Objection to form.

THE WITNESS: More than that. Practically computes that with the existing computing arsenal we had in a very reasonable amount of timing, hours or maybe no more than days, it can be computed.

BY ATTORNEY EKLEM:

Q. So could you -- I mean, so then what does it mean to allow one to practically compute predecessors or successors? Can you explain what that means?

A. It means with a small amount of resources, computing and money and small amount of time, you can do it.

Q. What's a small amount of time?

110

A. Minutes sometimes. But not years.

Q. And you're saying whether something is practical to compute depends on the time frame because technology changes?

A. The current time frame, yes. Practical could be different 100 years from today where we have, I don't know, quantum computers. You know, we're talking about this decade, more or less, or last decade at most.

Q. Okay. So let's go back to your declaration, please, and go to paragraph 86.

A. Okay. Thank you.

Q. Okay. You're there, Dr. Koc?

A. Yeah. Yes, I am.

Q. Thank you.

A. Yeah.

Q. And in the middle of the paragraph starts a sentence [as read]:

> **"The earliest version of DSS, which published in 1994, distinguishes between randomly generated and pseudorandomly generated integers (i.e., numbers)."**

And then you have a citation

111

there to Exhibit P to your declaration.

Do you see that?

A. Yeah.

Q. Okay. But you have in here quotations from that document --

A. Yeah.

Q. -- where it says [as read]:

> **"x equals a randomly or pseudorandomly generated integer. k equals a randomly or pseudorandomly generated integer."**

Do you see that?

A. Yes.

Q. So for purposes of DSA, random or pseudorandom is acceptable, right?

A. This is not standard. As you said, it was published in 1994, and a lot of things have changed since then.

Standards do not necessarily really tell you what key lengths to select and how much secure you will be, but it just makes the computational steps very clear.

As you can see, it says "random or pseudorandom," which means truly random or

112

zero random. We can use both.

But that's from 1994 until today, at 30 years as an expert. Not just myself, also Werner Schindler would tell you, for cryptography, you must select it randomly, truly randomly, period.

ATTORNEY EKLEM: Why don't we take a ten-minute break. I need to go through my notes here. I think we might be finished.

THE VIDEOGRAPHER: Now going off the video record. The time is 11:27 a.m.

- - -

(Whereupon, a short recess was taken.)

- - -

THE VIDEOGRAPHER: We are now going back on the video record. The time is 11:38 a.m.

ATTORNEY DESAI: Okay. I have a few -- sorry. Are you done?

ATTORNEY EKLEM: Almost.

ATTORNEY DESAI: Sorry. Sorry. Go ahead.

ATTORNEY EKLEM: Yes.

113

BY ATTORNEY EKLEM:

Q. Dr. Koc, did you have any conversations with counsel during the break about the substance of your testimony?

A. No.

ATTORNEY EKLEM: Okay. I have no further questions at this time.

ATTORNEY DESAI: Okay.

- - -

EXAMINATION

- - -

BY ATTORNEY DESAI:

Q. Dr. Koc, do you have your declaration?

A. Yes.

Q. Okay. Could you turn to paragraph 57.

A. Yes.

Q. So we're at page 23 for the screen --

A. Yeah.

Q. -- paragraph 57.

Okay. And in this paragraph, you state that [as read]:

> **"Both the standard Montgomery method and the**

114

'286 Patent method involve clearing the least significant portions of an unreduced operand."

Do you see that?

A. Yes.

Q. Okay. Now, Mr. Eklem asked you what "clearing" means, and I believe you said "cancelation."

Do you recall that testimony?

A. Yes.

Q. Okay. Is it your testimony that both the standard Montgomery method and the '286 Patent method used cancelation?

A. Yes.

ATTORNEY EKLEM: Objection. Leading.

ATTORNEY DESAI: Okay. I'm sorry.

BY ATTORNEY DESAI:

Q. So how are the least significant portions cleared in standard Montgomery reduction?

A. By adding m times n clears off the least significant word.

115

Q. When you say "clears off the least significant word," can you be more specific what you mean?

A. Makes it zero. Makes it zero, the least significant word.

Q. Okay. And how are the least significant portions cleared in the '286 Patent method?

A. By adding 2a -- a0 n prime 2 to the w.

Q. And if we go to -- if we go to paragraph 54, your declaration.

A. Yes.

Q. At the bottom of page 20, there is a reference to [as read]:

"MARA's proposed construction of 'replacement'"?

A. Yeah.

Q. Okay. And you see that the construction is [as read]:

"Add a modular equivalent of the operand's least significant word to the more significant words of the

116

operand such that the result can be shifted down to drop the least significant word."

Do you see that?

A. Yes.

Q. If you have an operand and you add a modular equivalent of the operand's least significant word, does that addition necessarily result in zeroing the least significant word of the operand?

A. No. It would depend. It has to be selected. Those multiplication -- multiplicative factor has to be correctly selected.

Q. Okay. Can we go to -- back to page 23. I want to just pull up that example you have on page 23.

A. Yes.

Q. Okay. Now, this is an example of the '286 Patent method; is that right?

A. Yes.

Q. Okay. And in Step 3, what's happening there?

A. The last two digits are -- according to the '286 Patent, are made little. That's

117

what it's done, yeah.

Q. Can you perform the '286 Patent method without zeroing the least significant word first?

A. I have tried that. And in the example, I can leave that 95 there and go ahead and add to it T0 n prime 10 to the w because that number is already -- has two zeros on the right. It doesn't touch the 95. 95 remains in place. The rest of the number is affected. And so you can go ahead and shift it to right, ignore 95, still have the correct result.

Q. Okay. So if we omit the zeroing Step 3, okay -- you understand?

A. Yes.

Q. -- and we do Step 4 now, that would mean you would do -- the addition would be 39195 plus 95 times 65 times 10 squared, right?

A. Right.

Q. And you could do the math yourself, but would you agree that the result of that, what I just stated, would be 656695?

Do you want to just confirm that?

A. True. Yes. Yes.

118

Q. So that would be an example of adding a modular equivalent of the operand's least significant word that does not result in zeroing the least significant word of the operand?

A. Indeed, correct.

Q. So we would have arrived at the same place in Step 5 when we shift the two digits right, and we did that without having added to zero the least significant word, right?

A. True. True.

Q. So unlike standard Montgomery, is it fair to -- is it fair to say that the '286 method does not require an addition that zero is the least significant word?

A. It doesn't.

ATTORNEY DESAI: I don't have any further questions. Thank you.

ATTORNEY EKLEM: Just a minute. We don't have to take a -- sorry. I was going to say we don't need to break. Just give me one second.

Just a quick follow-up.

- - -

EXAMINATION

119

- - -

BY ATTORNEY EKLEM:

Q. Dr. Koc, in the -- your counsel was just asking you about your example on page 23 of your declaration.

A. Yeah.

Q. As I understand it, the -- counsel was asking you about modifying that example such that in Step 3 this least significant word of T is not zeroed such that in Step 4 the T0 would be 39195, correct?

A. Yes.

Q. And so if you did that, you're saying that the answer at the very end would still come out to 87?

A. Yes, it would. Because all the temporary results would be the same as this example, and you would end up with 87.

Q. So help me understand a little bit.

You're saying that the temporary results -- you're saying that the temporary results would be the same as this example, meaning if you did Steps 1 through 8 at each step of Figure 7?

ATTORNEY DESAI: Objection.

120

Form.

THE WITNESS: So let me explain that to you. Look at Steps 3, 4, 5.

In one branch of computation, you zero the last two digits. You're at 095. Add T0 n prime 10 to the w.

BY ATTORNEY EKLEM:

Q. Uh-hum.

A. And so that way you get 656600. And you shift it right; you have 6566.

And in the other branch of computation, you don't zero 39195. You remain -- you keep 95.

Now, when you keep 95, you have 39195. Then add it to it, 95 times 65 times 100, doesn't touch the lower digits. Because that 100, whatever the product 65 times 95 is, that 100 makes it two zero on the right. It doesn't touch the 95. 95 remains in place, so the number becomes 656695.

Now, go ahead and shift it two digits to right, you get 6566s, which is the same as Step 5. This particular example is short. Really, 3, 4, 5 is the only three -- only step as needed. The 6, 7, 8 is not '286

121

regular steps. It's the Montgomery reduction step, because the '286 algorithm works that way. Defines itself to be multiple steps of Lambert, let's call it, because that was the inventor, Lambert reduction 3, 4, 5, another 3, 4, 5, another 3, 4, 5, but the number is bigger, modulus is bigger when all of them are finished, and you do a Montgomery and you have the result.

So what I'm saying is that for every 3, 4, 5 type of steps, results for the fifth step, at the end of fifth step, would be the same whether you erased that two digits or not erased two digits. So that way, when you enter the Montgomery step, it would enter at the same number and compute the same result, 87.

Q. So in that scenario, in this modified scenario we're talking about where you don't zero at Step 3, at Step 4, are you still adding a modular equivalent?

A. Writing the same number, you can. You write the same number, 95 times 65 times 100, and to the number that was -- whose last two digits was not zero.

122

Q. Okay. Got it.

ATTORNEY EKLEM: Okay. I have no further questions.

Dr. Koc, thank you for your time.

THE VIDEOGRAPHER: With that, we're concluding the deposition. The time on the record is 11:54 a.m.

THE COURT REPORTER: Can I get the orders for the record.

Mr. Eklem, I think we have a standing order.

Mr. Desai, would you like an immediate rough draft and an expedited copy?

ATTORNEY DESAI: Yes, please.

THE COURT REPORTER: And what would you like for the final?

ATTORNEY DESAI: We can take the final like Tuesday of next week.

THE COURT REPORTER: Okay. That's fine.

THE VIDEOGRAPHER: Okay.

- - -

123

(Whereupon, the deposition was concluded at 11:54 a.m.)

- - -

124

CERTIFICATE

I HEREBY CERTIFY that the proceedings, evidence and objections are contained fully and accurately in the stenographic notes taken by me upon the deposition of ÇETIN KAYA KOC, taken on 1/9/26 and that this is a true and correct transcript of same.

Jennifer Miller, RMR, CCR, CRR
and Notary Public

(The foregoing certification of this transcript does not apply to any reproduction of the same by any means unless under the direct control and/or supervision of the certifying reporter.)

125

Case: Malikie Innovations Ltd., et al. vs Mara Holdings, Inc.
Witness Name: Dr. Çetin Kaya Koç
Deposition Date: 01/09/2026

Please be advised that the transcript in the above referenced matter is now complete and ready for signature. The deponent may come to this office to sign the transcript, a copy may be purchased for the witness to review and sign, or the deponent and/or counsel may waive the option of signing. Please advise us of the option selected. Please forward the errata sheet and the original signed signature page to counsel noticing the deposition, noting the applicable time period allowed for such by the governing Rules of Procedure. If you have any questions, please do not hesitate to call our office at (202)-232-0646.

Sincerely,
Digital Evidence Group

Digital Evidence Group, L.L.C.
1730 M Street, NW, Suite 812
Washington, D.C. 20036
(202) 232-0646

SIGNATURE PAGE
Case: Malikie Innovations Ltd., et al. vs Mara Holdings, Inc.
Witness Name: Dr. Çetin Kaya Koç
Deposition Date: 01/09/2026

I do hereby acknowledge that I have read and examined the foregoing pages of the transcript of my deposition and that:

(Check appropriate box):

( ) The same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

( ) Except for the changes noted in the attached Errata Sheet, the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

______________ ___________________________
DATE WITNESS SIGNATURE

______________ ___________________________
DATE NOTARY

Errata Sheet
NAME OF CASE: Malikie Innovations Ltd., et al. vs Mara Holdings, Inc.
DATE OF DEPOSITION: 01/09/2026
NAME OF WITNESS: Dr. Çetin Kaya Koç
Reason Codes: 1. To clarify the record.
2. To conform to the facts.
3. To correct transcription errors.

Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________
Page _____ Line ______ Reason ______
From _______________________ to _______________________

____
CETIN KOC